(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 June 2001 (07.06.2001)

PCT

(10) International Publication Number
WO 01/41392 A2

(51) International Patent Classification[7]: H04L 29/00

(21) International Application Number: PCT/SG00/00192

(22) International Filing Date:
17 November 2000 (17.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9905842-2 18 November 1999 (18.11.1999) SG

(71) Applicant *(for all designated States except US)*: **SINGAPORE TELECOMMUNICATIONS LIMITED** [SG/SG]; 31 Exeter Road, Comcentre, Singapore 239732 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHONG, Kai, Yew, Paul** [SG/SG]; 3 Rhu Cross, #04-15 Costa Rhu Condominium, Singapore 437433 (SG). **FOONG, Sui, Jin** [MY/SG]; 115 Bedok Ria Crescent, Singapore 489925 (SG). **TEO, Keng, Wui, Daniel** [SG/SG]; Blk 725, 6 Ang Mo Kio Avenue, #08-4142, Singapore 560725 (SG). **THIA, Kok, Soon** [SG/SG]; Blk 99, Old Airport Road, #07-189, Singapore 390099 (SG). **TAN, Boon, Tiong** [SG/SG]; 20 Amber Road, #11-02 King's Mansion Blk C, Singapore 439869 (SG). **YAP, Tye, San** [SG/SG]; 10 Flora Road, #09-07, Singapore 509729 (SG).

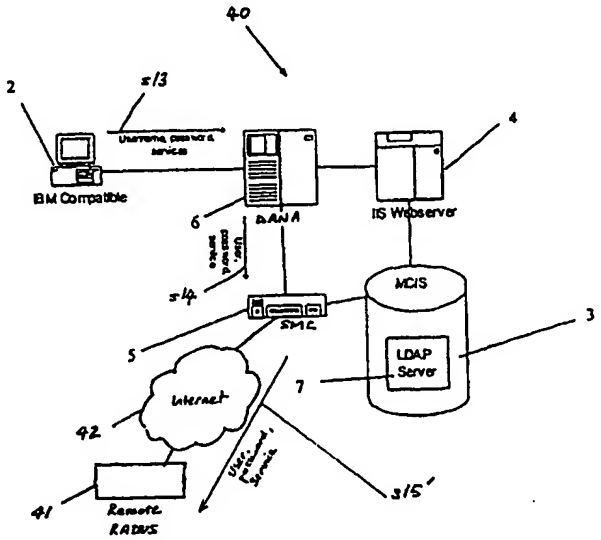
(74) Agent: **ALLEN & GLEDHILL**; 36 Robinson Road, #18-01 City House, Singapore 068877 (SG).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: VIRTUAL PRIVATE NETWORK SELECTION



(57) Abstract: A system enables the selective connection of a data terminal (2) to one of a plurality of VPNs (20-24) formed within a public telecommunication network. A data storage computer (7) within the system stores users identity information indicative of the identity of authorized users to one or more of said VPNs, and VPN authorisation information indicative of those VPNs that each authorised user is authorised to use. Retrieval means, such as a web server (4), send a user identifier indicative of a selected authorised user to the data storage computer and retrieve a list of VPNs accessible by the selected authorised user from the first data storage computer. The data terminal includes a display for presenting the list of VPNs, and selection means for accepting the selection at the data terminal of one of the virtual private networks. The system includes authenticating means, such as a RADIUS client/server, for authenticating the identity of said selected authorised user, the data terminal being connected to the selected VPN if the authentication is successful.

WO 01/41392 A2

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

VIRTUAL PRIVATE NETWORK SELECTION

The present invention relates generally to virtual private networks, and more particularly to a method and system for selectively connecting a remote data terminal to one or more virtual private networks using a customised client or a web browser.

A virtual private network (VPN) is a private data network that is formed within and makes use of a larger public telecommunication network, such as the Internet, or a larger private telecommunications network. Use of a VPN provides companies with the same capabilities as a system of owned and leased telecommunication lines and exchanges, but at a much lower cost by using the shared public infrastructure rather than a private one. Privacy is maintained in a VPN through use of a tunnelling protocol, by which data is encrypted before it is sent through the public network and decrypted at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. VPNs therefore make it possible to have the same secure sharing of public resources. Companies today are looking at using VPNs for both Extranets and wide-area Intranets.

It is envisaged that various services requiring the transport of video, audio or data information between nodes within a VPN will be offered in the near future. Examples of such services include financial and banking services, as well as traditional telephony services. The proliferation of VPN-based services will no doubt result in individual users subscribing to and using several such services.

It would therefore be desirable to provide a method and system for facilitating the access of users to VPNs offering such services.

With that in mind, one aspect of the present invention provides a method for selectively connecting a data terminal to one of a plurality of VPNs, said

VPNs being formed within a telecommunication network, the method including the steps of:

(a) storing in a first data storage computer (i) user identity information indicative of the identity of authorized users to one or more of said VPNs and (ii) VPN authorisation information indicative of those VPNs that each authorized user is authorized to use;

(b) connecting said data terminal to the telecommunication network;

(c) sending a user identifier indicative of a selected one of said authorized users to said first data storage computer;

(d) retrieving a list of VPNs accessible by the selected authorized user from the first data storage computer;

(e) presenting said list of VPNs at said data terminal;

(f) accepting the selection at said data terminal of one of said virtual private networks;

(g) authenticating the identity of said selected authorized user; and

(h) if step (g) is successful, connecting said data terminal to the selected VPN.

The telecommunication network may be a public telecommunications network, such as the Internet. The data terminal may be connected at step (b) to the Internet with a public IP address. Alternatively, the data terminal may be connected at step (b) to a private telecommunications network, with the data terminal being connected with a private IP address. In both cases the IP address of the data terminal may be changed, at step (h), to an IP address with access to the selected VPN.

The connection of the data terminal to the public telecommunication network may be carried out in step (a) by a Remote Access Server.

The user identifier may be sent from the data terminal to the first data storage computer in step (b) via a Web Server.

A Web Browser may be installed in the Data Terminal to enable the entry and sending of said user identifier.

The list of VPNs retrieved from the first data storage computer in step (c) may be transmitted to the Data Terminal by the Web Server.

The list of VPNs may be displayed at the Data Terminal by the Web Browser.

The authenticating of the identity of the selected authorized user in step (g) may be performed by a RADIUS/LDAP client in conjunction with a RADIUS/LDAP server, said RADIUS/LDAP server storing user authentication information.

The first data storage computer acts as said RADIUS/LDAP server.

Alternatively, a second data storage computer may be remotely connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS/LDAP server. The second data storage computer may connectable to said RADIUS/LDAP client via the Internet.

In another embodiment, the second data storage computer may be connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS/LDAP server, both second data storage computer and said RADIUS/LDAP client being remotely connectable to said Remote Access Server. The RADIUS/LDAP client may be connectable to said Remote Access Server via the Internet.

Another aspect of the invention provides a system for selectively connecting a data terminal to one of a plurality of VPNs, said VPNs being formed within a telecommunication network, the system comprising:

a first data storage computer for storing (i) user identity information indicative of the identity of authorized users to one or more of said VPNs and (ii) VPN authorisation information indicative of those VPNs that each authorized user is authorized to use,

connection means for connecting said data terminal to the telecommunication network;

retrieval means for sending a user identifier indicative of a selected authorized user to said first data storage computer and retrieving a list of VPNs accessible by the selected authorized user from the first data storage computer,

said data terminal including

display means for presenting said list of VPNs, and

selection means for accepting the selection at said data terminal of one of said virtual private networks, the system further comprising

authenticating means for authenticating the identity of said selected authorized user,

said connection means acting to connect said data terminal to the selected VPN if the authentication is successful.

The following description refers in more detail to the various features of the invention. To facilitate an understanding of the invention, reference is made in the description to the accompanying drawings where various embodiments of the method and system for selectively connecting a remote data terminal to one or more virtual private networks are illustrated. It is to be understood, however, that the invention is not limited to the preferred embodiments as illustrated in the drawings.

In the drawings:

Figures 1 to 5 are schematic block diagrams illustrating a first embodiment of a system for selectively connecting a remote terminal to one of a plurality of VPNs, and the flow of information between various elements of that system during operation;

Figures 6 and 7 are schematic block diagrams illustrating a second embodiment of a system for selectively connecting a remote terminal to one of a plurality of VPNs;

Figure 8 is a schematic block diagram illustrating a third embodiment of a system for selectively connecting a remote terminal to one of a plurality of VPNs; and

Figures 9 to 11 are representations of graphical displays provided to the user of the data terminal of the systems of Figures 1 to 8 during operation.

Referring now to Figures 1 to 5, there is shown generally a system 1 for selectively connecting a data terminal 2 to one of a plurality of virtual private networks (VPNs). The data terminal 2 may consist of a personal

computer and modem to enable connection of the personal computer to the public telephony network. The system 1 includes a Data File Server 3, a Web Server 4, a Remote Authentication Dial-In User Service (RADIUS) communications device 5 and a Remote Access Server (RAS) 6. The File Server 3 includes a Data Storage Computer 7.

The RAS 6 is deployed at a local telephony exchange in which the data terminal 2's virtual circuits aggregates into, and manages the Internet access for the data terminal 2 and other data terminals and devices connecting to the Internet via that telephony exchange. Examples of RAS's that are suitable for use with the present invention are the Redback™ Subscriber Management System 1000 and the Alcatel™ Data Application Network Adapter (DANA).

The Web Server 4 provides World Wide Web services on the Internet to the data terminal 2 and other terminals and devices connected to the Internet. It may include hardware, an operating system, Web server software, TCP/IP protocols and Web site content (Web pages). Alternatively, the Web Server 4 may simply comprise software installed on a host computer that performs these services. The software acts to accepts requests from a Web browser installed in the data terminal 2 to download HTML pages and images, and also to execute related server-side scripts that automate functions such the searching of the LDAP data storage computer. An example of this latter type of Web Server is the Microsoft™ Internet Information Server. A mini-Web browser suitable for installation on the data terminal 2 which can adapted to implement the required functionality may be readily developed by a skilled person in the computing/telecommunications field.

RADIUS is a proposed Internet Engineering Task Force (IETF) standard and uses a client/server protocol and software to enable remote access servers, such as the RAS 6, to communicate with a central server, such as the Data Storage Computer 7, so as to authenticate the identity of dial-in users and authorize their access to a requested service or system. All user authentication and network service access information is located on the Data Storage Computer 7, which acts as the RADIUS/LDAP server. The RADIUS

communications device 5 (RADIUS client) and sends authentication requests to the Data Storage Computer 7 (RADIUS/LDAP server) and acts on responses sent back by the server. One example of a RADIUS communications device 5 suitable for use with the present invention is the Alcatel™ Service Management Centre (SMC).

The Data Storage Computer 7 acts to store and retrieve user information and authorisation information. The Data Storage Computer 7 may operate in accordance with the Lightweight Directory Access Protocol (LDAP), a client-server protocol developed for accessing directory service information. One example of a Data Storage Computer 7 suitable for use with the present invention is the Microsoft™ Commercial Internet System (MCIS) with a LDAP server. MCIS has been developed for use by Commercial Service Providers (CSPs), such as Internet and on-line service providers, and includes an LDAP data storage computer.

The operation of the system 1 will now be described. Initially, VPN identification information indicative of several VPNs to which users may subscribe or otherwise be provided with access to is stored in the Data Storage Computer 7. In addition, user identity information indicative of the identity of users who are authorized to access one or more of those VPNs, and VPN authorisation information indicative of those VPNs which each user is authorized to access is stored in the Data Storage Computer 7. The Data Storage Computer 7 may also store user authentication information, such as a user name and a user password, for each authorised user to enable authentication of the identity of that user. At least some of the data stored in the Data Storage Computer 7 may be common to both the user identity information and the user authentication information.

When power is provided to the Data Terminal 2, an installed dialer program is run to cause the Data Terminal's modem to dial the RAS 6 over a Permanent Virtual Circuit, such encapsulating an Ethernet or a PPP connection, to be established between the Data Terminal 2 and the RAS 6. Once the dialer program has been run, an IP address is assigned to the Data

Terminal 2 by the RAS 6 (step s1), effectively connecting the Data Terminal 2 to the public telecommunication network, and a Hyper Text Mark-up Language (HTML) page is retrieved from the Web Server 4 (step s2).

The HTML page is displayed to the user by the mini-Browser installed at the Data Terminal 2 (step s3). An example of such an HTML page is shown in Figure 9. The HMTL page includes a field 10 for the entry of a user's name (step s4) or other user identifier to identify the user to the RAS 6 or to the Web Server 4 accessed by the RAS 6. Optionally, a cookie may be set in the Data Terminal 42 so that the Web Server 4 is able to provide the HTML page for display by the mini-Browser with an expected user name inserted in the field 10. The HTML page may contain an ActiveX object that logs the user out of any previous VPN to which the Data Terminal 2 is connected. If ActiveX is not supported by the mini-Browser platform, the HTML page may display a text message to the user instructing the user to log out of any current VPN.

Once the user name is sent to the RAS 6 or the Web Server 4 (step s5), or alternatively, once the cookie containing the user's name is submitted, the Web Server 4 sends a query (step s6) to the Data Storage Computer 7 to retrieve from the stored user information and VPN authorisation information a list of those VPNs accessible to the identified user. The list of accessible VPNs is transmitted to the Web Server 4 (step s7).

The Web Server 4 then dynamically creates a customized HTML page containing the list of VPNs accessible to the user, and transmits this HTML page to the RAS 6 and onto the Data Terminal 2 (step s8). This HTML page is displayed by the mini-Browser installed in the Data Terminal 2 (step s9). An example of such an HTML page is shown in Figure 10. The list of accessible VPNs is displayed on this page as a series of icons 20 to 24, each of which corresponds to a different one of the VPNs accessible to the identified user. The VPN that the user wishes to use is then selected by using a mouse associated with the personal computer of the Data Terminal to position a cursor 25 over the icon corresponding to the selected VPN (step s10).

Upon selection of the desired VPN, the mini-Browser acts to display a further HTML page to the user (step s11). The HTML page, an example of which is shown in Figure 11, includes a field 30 for the entry of a user password (step 12). The user name, the selected VPN and the entered password are then submitted to the RAS 6 (step s13), and forwarded to the RADIUS communications device 5 (step 14). An attempt is then made to authenticate the identity of the user and whether or not the selected VPN is accessible to that user through a series of communications between the RADIUS/LDAP communications device 5 - acting as RADIUS client - and the Data Storage Computer 7 – acting as RADIUS/LDAP server – during which the user name, selected VPN and password are compared to the user authentication information stored in the Data Storage Computer 7 (step s15).

If the user's identity and access to the selected VPN are authenticated, an authentication message is sent to the RADIUS/LDAP Communications device 5 (step s16) and forwarded to the RAS 6 (step s17). The RAS 6 then changes the IP address of the Data Terminal 2 to an IP address with access to the selected VPN (step s18) and displays a "User Connected" message to the user via the mini-Browser. The mini-Browser can then be minimized until the user wishes to change VPN or disconnect.

If the user reactivates the dialer program installed in the Data Terminal 2, the user is automatically disconnected from the current VPN and presented with the VPN Service Selection page shown in Figure 10. The user may also be disconnected if the RAS 6 detects zero or a very low level of network activity by the user.

The RADIUS/LDAP Communication device 5 may also collect accounting data, such as the user name, login time, logout time and VPN used.

For each scenarios described, the presentation of a login web page, such as that shown in Figure 10, may not be bypassable. That is to say, a client cannot gain access to any of the VPNs 20 to 24 without first obtaining a page presenting the choices of subscribed VPNs. Moreover, on successful connection to one of the VPNs 20 to 24, the user may be presented with a

VPN-specific welcome page which also may not be bypassable. The control of the VPN-specific welcome page may be provided by the remote access server (RAS) 6, the RADIUS communication device 5, or the Data Storage Computer 7

There will now be described a first variant of the system 1. In Figures 6 and 7, there is shown generally a system 40 for selectively connecting a data terminal 2 to one of a plurality of virtual private networks (VPNs), which includes the Data Storage Computer 7, Web Server 4, RADIUS/LDAP communications device 5 and a RAS 6 of Figures 1 to 5. In the system 40, however, user authentication is partially handled at a remote location from the RAS 6. In that regard, the system 40 includes a further Data Storage Computer 41, acting as a remote RADIUS server, which is connectable to the RADIUS/LDAP communications device 5 by a telecommunications network 42, such as the Internet. The remote RADIUS server 41 stores the user authentication information, whilst the RADIUS/LDAP communications device 5 acts here as a RADIUS proxy and forwards data packets for processing to the remote RADIUS server 41.

In operation, steps s1 to s14 are carried out in the same manner as described in relation to Figures 1 to 5. However, once the user name, selected VPN and password have been forwarded to the RADIUS/LDAP communications device 5 at step s14, a data packet containing this information is sent to remote RADIUS server 41 and the identity of the user authenticated (step s15').

If the user's identity and access to the selected VPN are authenticated, a data packet containing an authentication message is sent to the RADIUS/LDAP Communications device 5 (step s16'). Thereafter, the system 40 operates in accordance with steps s17 and s18 as described previously.

Figure 8 illustrates a second variant of the system 1. In this Figure, there is shown a system 50 for selectively connecting a data terminal 2 to one of a plurality of virtual private networks (VPNs), which again includes the Data Storage Computer 7, Web Server 4, RADIUS/LDAP communications

device 5 and a RAS 6 of Figures 1 to 5. In this case, however, a Remote Access Server which is also a RADIUS client device 51 and another Data Storage Computer 52 remotely connected to the RAS 6 by a telecommunications network, such as the Internet, are also provided. The Data Storage Computer 52, which may be a RADIUS server, stores the user authentication information and together with the external RADIUS client device 51 acts to entirely handle user authentication at a remote location from the RAS 6.

The system 50 operates in accordance with steps s1 to s13 as described in relation to Figures 1 to 5. However, in this case once the user name, selected VPN and password have been forwarded to the RAS 6 at step s13, the RAS 6 merely forwards an entire Point-to-Point Protocol (PPP) packet containing the user name, selected VPN and password over a secure tunneling protocol - such as Layer 2 Tunneling Protocol (L2TP) – to the RADIUS client device 51 (step s14'').

An attempt is then made to authenticate the identity of the user and whether or not the selected VPN is accessible to that user through a series of communications between the RADIUS client device 51 and the Data Storage server 52 – – during which the user name, selected VPN and password are compared to the user authentication information stored in the server 52.

If the user's identity and access to the selected VPN are authenticated, a PPP packet containing the IP address to the selected VPN is sent to Data Terminal 2 (step s15''). Thereafter, the system 50 operates in accordance with step s18 as described previously.

Finally, it is to be understood that various modifications and/or additions may be made to the above-described method and system without departing from the ambit of the present invention as defined in the claims appended hereto.

CLAIMS

The claims defining the invention are as follows:

1. A method for selectively connecting a data terminal to one of a plurality of VPNs, said VPNs being formed within a telecommunication network, the method including the steps of:

(a) storing in a first data storage computer (i) user identity information indicative of the identity of authorized users to one or more of said VPNs and (ii) VPN authorisation information indicative of those VPNs that each authorized user is authorized to use;

(b) connecting said data terminal to the telecommunication network;

(c) sending a user identifier indicative of a selected one of said authorized users to said first data storage computer;

(d) retrieving a list of VPNs accessible by the selected authorized user from the first data storage computer;

(e) presenting said list of VPNs at said data terminal;

(f) accepting the selection at said data terminal of one of said virtual private networks;

(g) authenticating the identity of said selected authorized user; and

(h) if step (g) is successful, connecting said data terminal to the selected VPN.

2. A method according to claim 1, wherein

said telecommunication network is a public telecommunications network, such as the Internet.

3. A method according to claim 2, wherein

at step (b), the data terminal is connected to the public telecommunications network with a public IP address; and

at step (h), the IP address of the data terminal is changed to an IP address with access to the selected VPN.

4. A method according to claim 1, wherein said telecommunication network is a private telecommunications network.

5. A method according to claim 4, wherein at step (b), the data terminal is connected to the private telecommunications network with a private IP address; and at step (h), the IP address of the data terminal is changed to an IP address with access to the selected VPN.

6. A method according to any one of the preceding claims, wherein the connection of the data terminal to the public telecommunication network is carried out in step (a) by a Remote Access Server.

7. A method according to any one of the preceding claims, wherein the user identifier is sent from the data terminal to the first data storage computer in step (b) via a Web Server.

8. A method according to claim 7, wherein a Web Browser is installed in the Data Terminal to enable the entry and sending of said user identifier.

9. A method according to either of claims 7 or 8, wherein the list of VPNs retrieved from the first data storage computer in step (c) are transmitted to the Data Terminal by the Web Server.

10. A method according to claim 9, wherein the list of VPNs are displayed at the Data Terminal by the Web Browser or customised client.

11. A method according to any one of the preceding claims, wherein the authenticating of the identity of the selected authorized user in step (g) is performed by a RADIUS/LDAP client in conjunction with a RADIUS/LDAP server, said RADIUS/LDAP server storing user authentication information.

12. A method according to claim 10, wherein said first data storage computer acts as said RADIUS/LDAP server.

13. A method according to claim 11, wherein a second data storage computer is remotely connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS/LDAP server.

14. A method according to claim 13, wherein said second data storage computer is connectable to said RADIUS/LDAP client via the Internet.

15. A method according to claim 11 when dependant upon claim 6, wherein a second data storage computer is connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS/LDAP server, both second data storage computer and said RADIUS/LDAP client being remotely connectable to said Remote Access Server.

16. A method according to claim 15, wherein said RADIUS/LDAP client is connectable to said Remote Access Server via the Internet.

17. A system for selectively connecting a data terminal to one of a plurality of VPNs, said VPNs being formed within a telecommunication network, the system comprising:

a first data storage computer for storing (i) user identity information indicative of the identity of authorized users to one or more of said VPNs and (ii) VPN

authorisation information indicative of those VPNs that each authorized user is authorized to use,

connection means for connecting said data terminal to the telecommunication network;

retrieval means for sending a user identifier indicative of a selected authorized user to said first data storage computer and retrieving a list of VPNs accessible by the selected authorized user from the first data storage computer, said data terminal including

display means for presenting said list of VPNs, and

selection means for accepting the selection at said data terminal of one of said virtual private networks, the system further comprising

authenticating means for authenticating the identity of said selected authorized user,

said connection means acting to connect said data terminal to the selected VPN if the authentication is successful.

18. A system according to claim 17, wherein

said telecommunication network is a public telecommunications network, such as the Internet.

19. A system according to claim 18, wherein

said data terminal is connected to the public telecommunications network with a public IP address,

said connection means acting to change the IP address of the data terminal to an IP address with access to the selected VPN if the authentication is successful.

20. A system according to claim 17, wherein

said telecommunication network is a private telecommunications network.

21. A system according to claim 20, wherein

said data terminal is connected to the private telecommunications network with a private IP address,

said connection means acting to change the IP address of the data terminal to an IP address with access to the selected VPN if the authentication is successful.

22. A system according to any one of claims 17 to 21, wherein said connection means include a Remote Access Server.

23. A system according to any one of claims 17 to 22, wherein said retrieval means include a Web Server connected to the data terminal and the central database via the Internet.

24. A system according to claim 23, wherein said display and selection means include a Web Browser or customised client is installed in the Data Terminal.

25. A system according to any one of claims 17 to 24, wherein said authenticating means includes a RADIUS/LDAP client acting in conjunction with a RADIUS/LDAP server, said RADIUS/LDAP server storing user authentication information.

26. A system according to claim 25, wherein said first data storage computer acts as said RADIUS/LDAP server.

27. A system according to claim 25, wherein a second data storage computer is remotely connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS server.

28. A system according to claim 27, wherein said second data storage computer is connectable to said RADIUS/LDAP client via the Internet.

29. A system according to claim 25 when dependant upon claim 22, wherein a second data storage computer is connectable to said RADIUS/LDAP client, said second data storage computer acting as said RADIUS/LDAP server, both second data storage computer and said RADIUS/LDAP client being remotely connectable to said Remote Access Server.

30. A system according to claim 29, wherein said RADIUS/LDAP client is connectable to said Remote Access Server via the Internet.

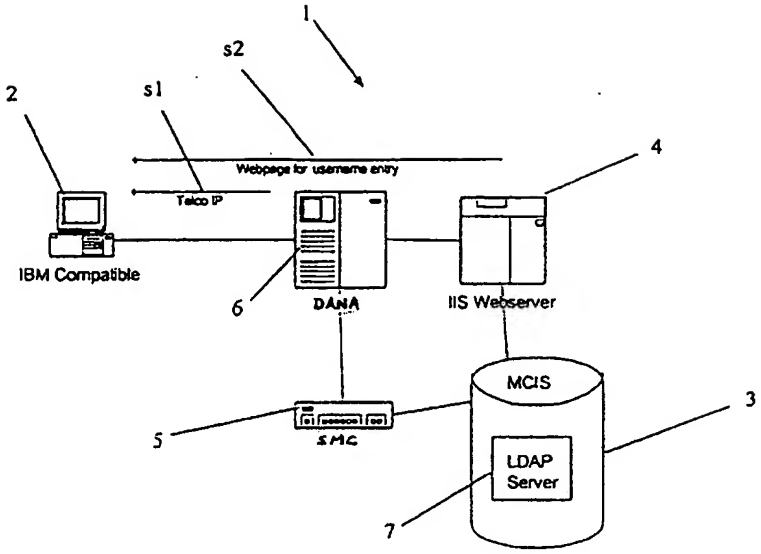

1
s2
s1
2
Webpage for username entry
Telco IP
4
IBM Compatible
6
DANA
IIS Webserver
MCIS
3
5
SMC
LDAP
Server
7

Figure 1

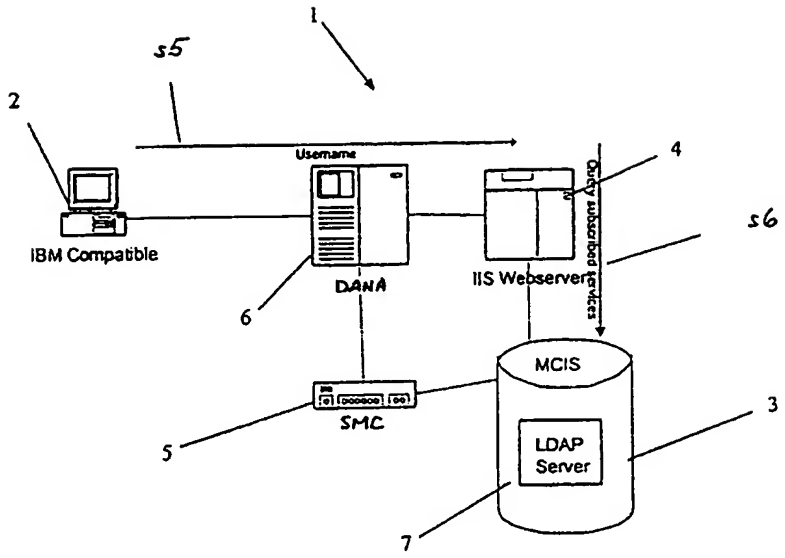

1
s5
2
Username
4
s6
IBM Compatible
DANA
IIS Webserver
Query published objects
6
MCIS
3
SMC
5
LDAP Server
7

Figure 2

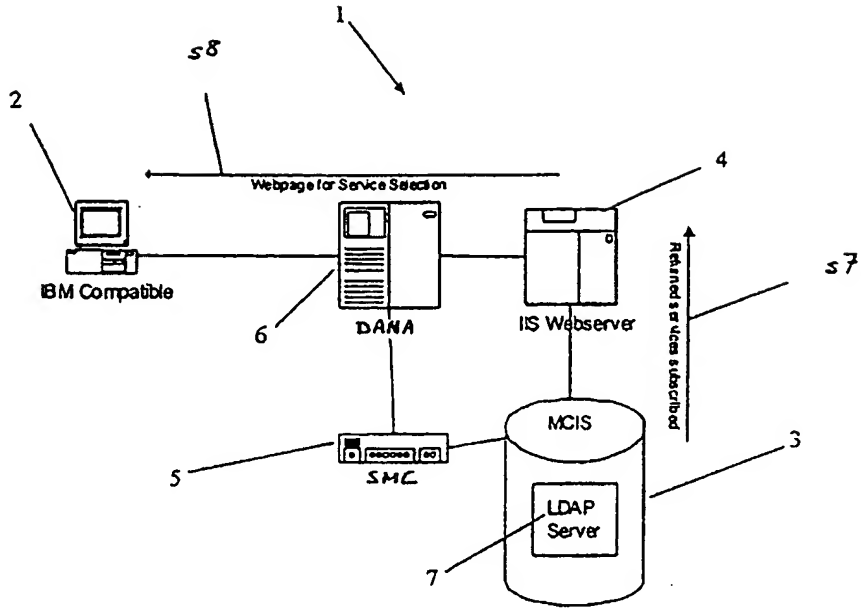

1
s8
2
Webpage for Service Selection
4
IBM Compatible
6
DANA
IIS Webserver
s7
Returned services subscribed
MCIS
3
5
SMC
LDAP Server
7

Figure 3

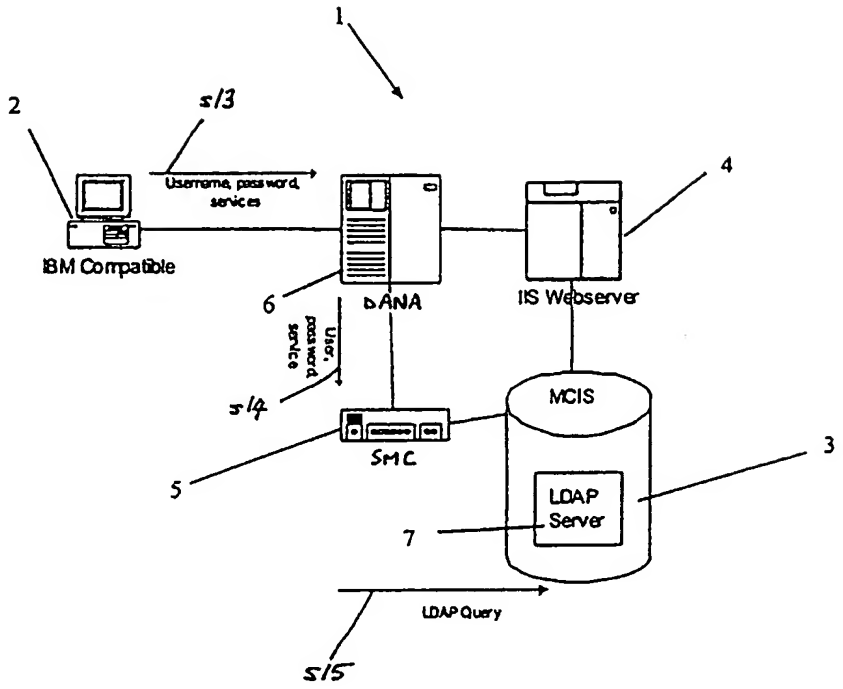

1
2
s13
Username, password, services
IBM Compatible
bANA
IIS Webserver
4
6
User, password, status
s14
SMC
5
MCIS
3
LDAP Server
7
LDAP Query
s15

Figure 4

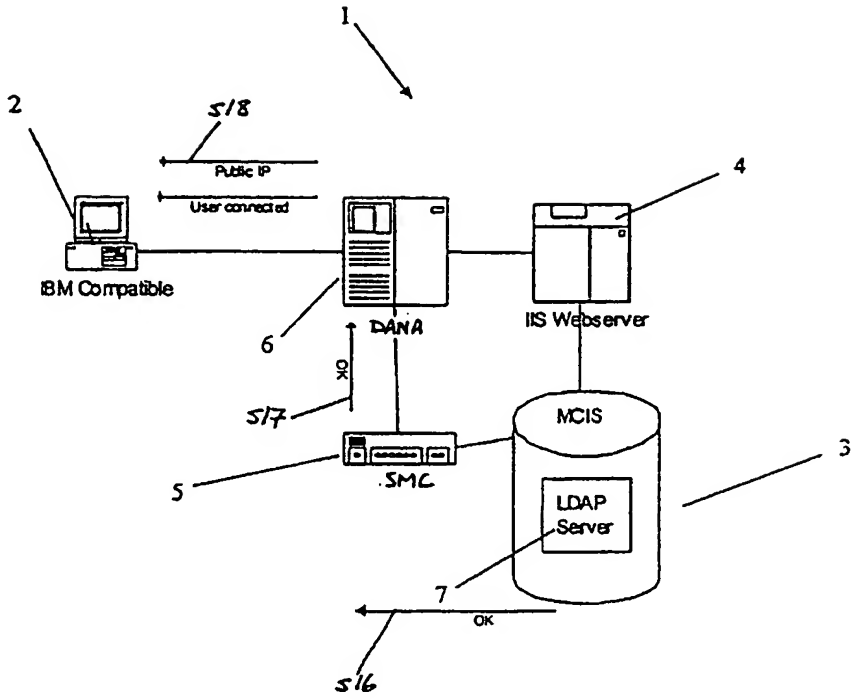

1
2
S18
Public IP
User connected
4
IBM Compatible
6
DANA
IIS Webserver
OK
S17
MCIS
3
5
SMC
LDAP
Server
7
OK
S16

Figure 5

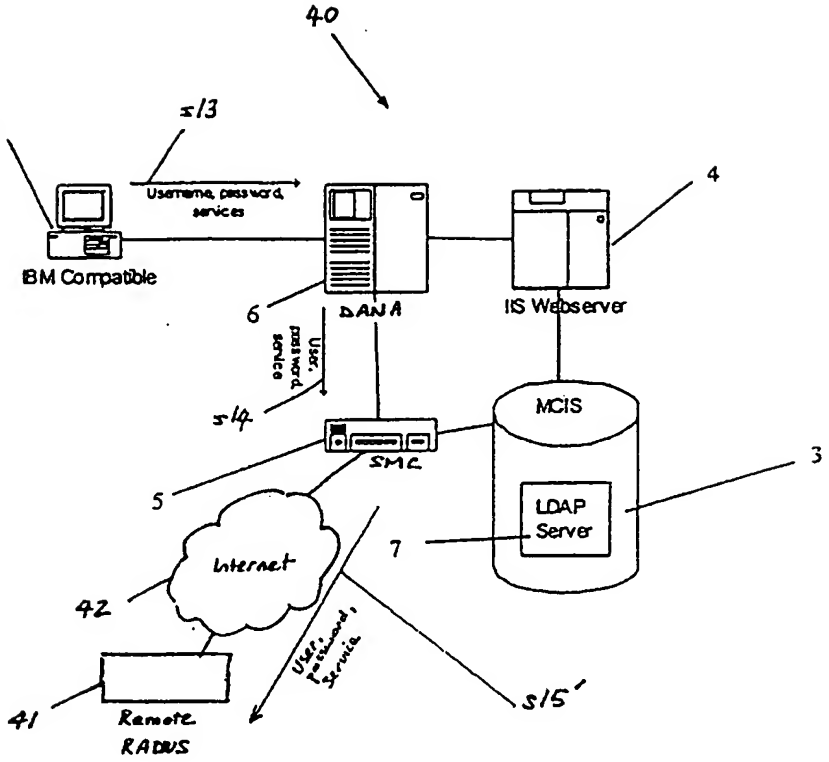

40
2
s13
Username, password, services
IBM Compatible
DANA
IIS Webserver
4
6
Username, password, service
s14
SMC
MCIS
3
5
LDAP Server
7
Internet
42
User, password, service
s15'
41
Remote RADIUS

Figure 6

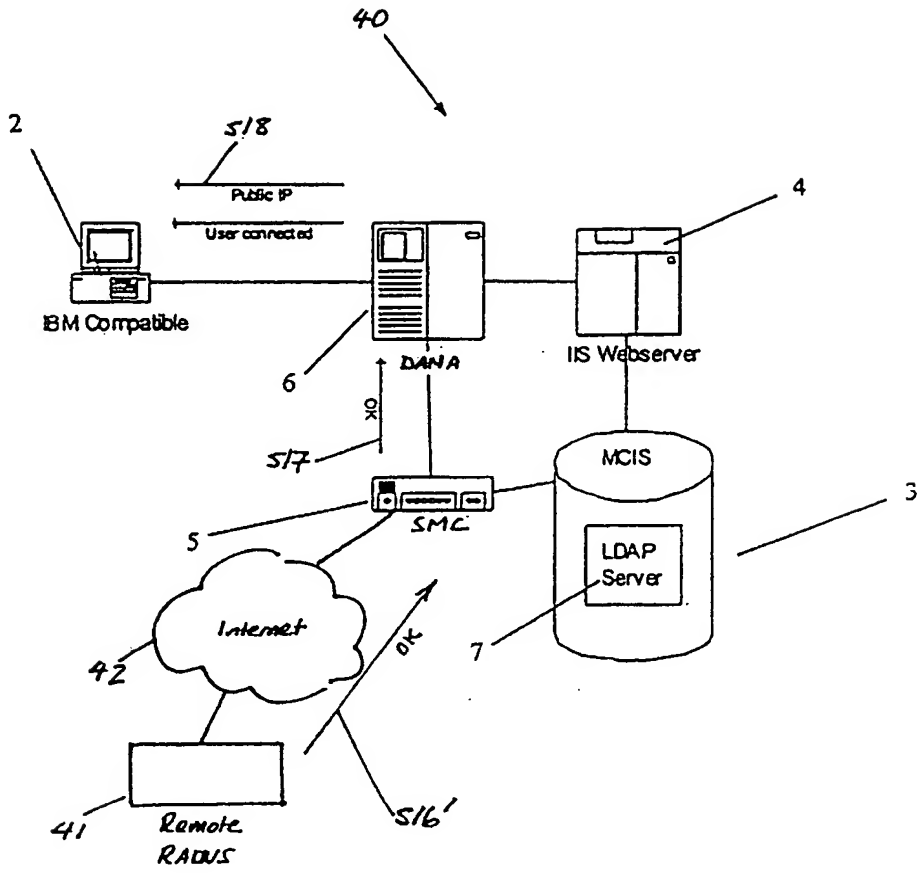

40
2
518
Public IP
User connected
4
IBM Compatible
DANA
IIS Webserver
6
OK
517
MCIS
3
SMC
5
LDAP
Server
Internet
OK
7
42
41
Remote
RADIUS
516'

Figure 7

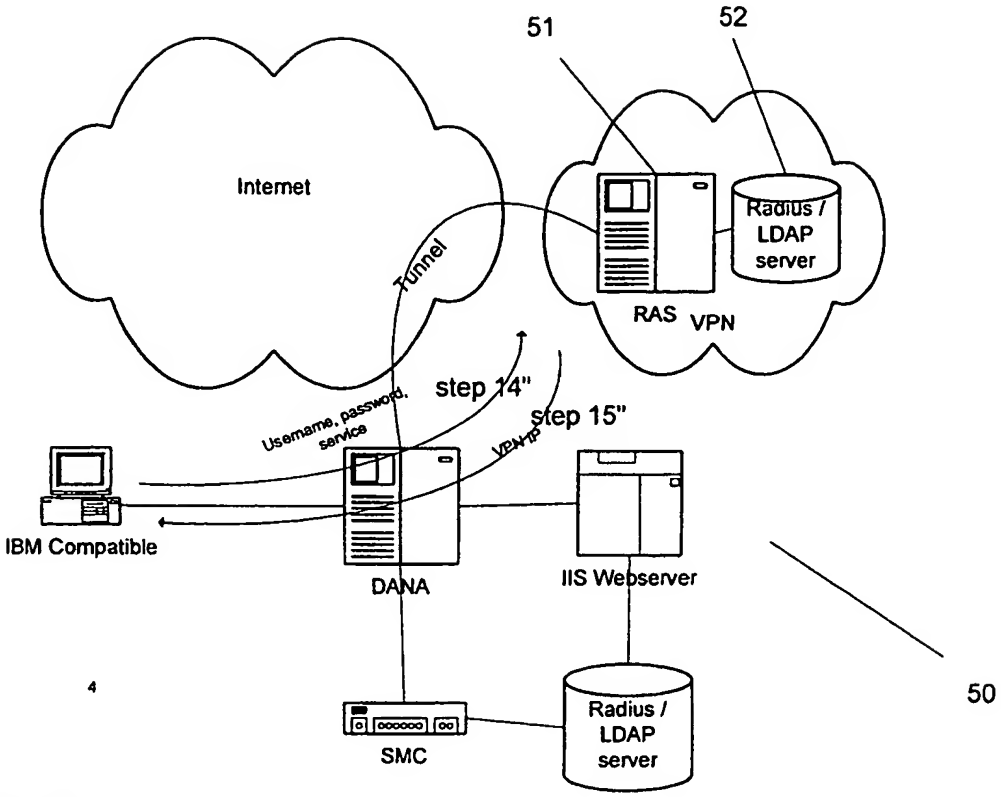

51
52
Internet
Tunnel
Radius / LDAP server
RAS
VPN
step 14"
step 15"
Username, password, service
VPN IP
IBM Compatible
DANA
IIS Webserver
4
50
SMC
Radius / LDAP server

Figure 8

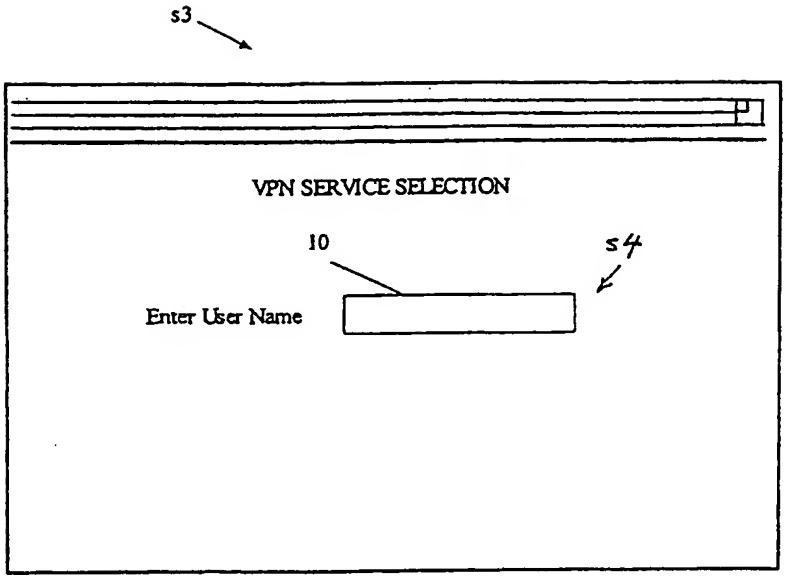


Figure 9

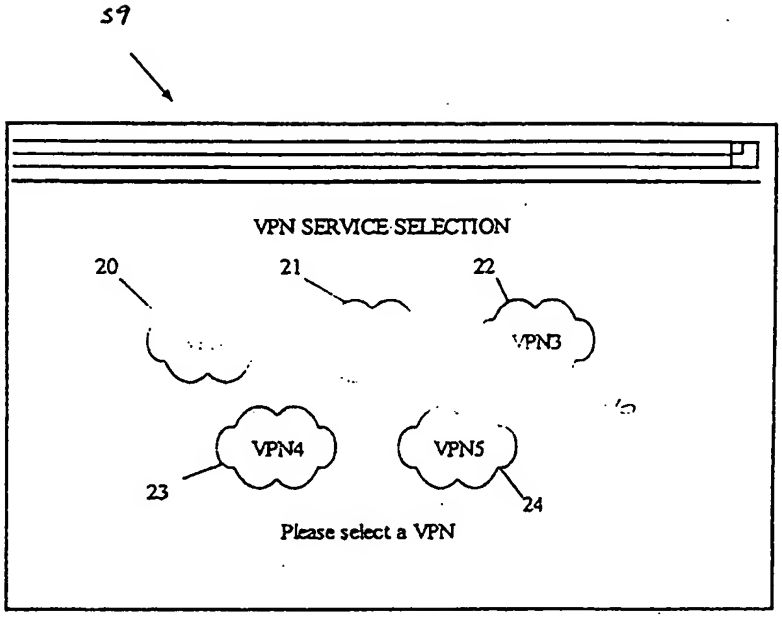

59
VPN SERVICE SELECTION
20
21
22
VPN3
VPN4
VPN5
23
24
Please select a VPN

Figure 10

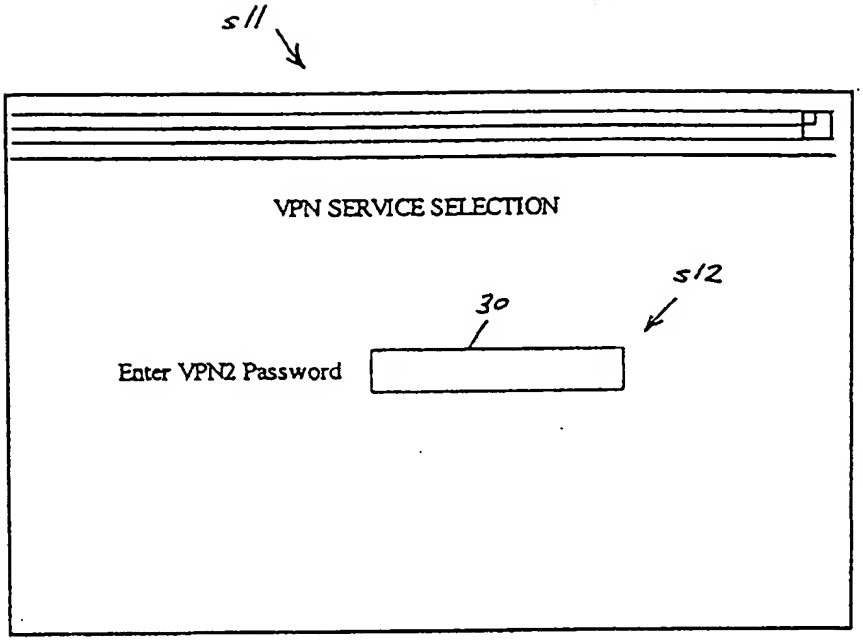


Figure 11